Kako ukloniti Sirefef (ZeroAccess)?

Pitanje

- ESET program detektira prijetnju Win32/Sirefef, Patched.b.gen, ili Conedex
- Vjerujete da je računalo inficirano lažnim antivirusnim programom kao što je npr: “Open Cloud Security”
- Dobivate poruku “Pogreška pri komunikaciji s jezgrom” (eng: “Error communicating with kernel”)

Detalji

Ovaj malware poznat je i kao “ZeroAccess” ili “Max++” i ESET detektira sve varijante ove prijetnje kao Win32/Sirefef.

Odgovor

I – Preuzmite ESETSirfefEVCleaner

Kliknite na link ispod kako bi preuzeli alat ESETSirfefEVCleaner.

Preuzmite ESET Sirefef Cleaner

Spremite datoteku na Desktop i nastavite na dio II.

Važno!

Novije varijante Sirefef malwarea mogu spriječiti download ESETSirefefEVCleanera. To možete prepoznati po ovoj poruci pogreške:

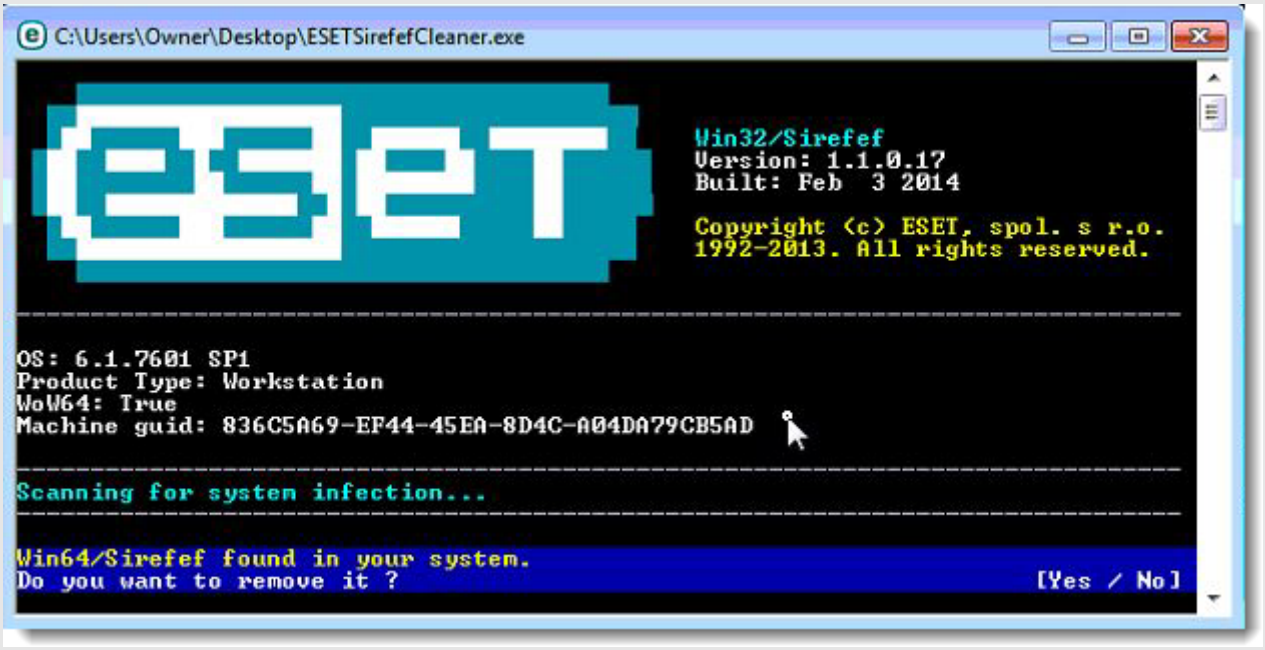
Unable to download: “ESETSirefefCleaner.exe contained a virus and was deleted”

Ako ne možete provesti download tog alata slijedite ove upute:

1. Kliknite na Start → Computer → Local Disk (C:) → Program Files.
2. Desnom tipkom miša kliknite na mapu Windows Defender i iz kontekstnog menija odaberite Rename.
3. Dodajte jedinstvenu varijaciju (dodatak) na to ime, kao što je .old (na primjer, Windows Defender.old).
4. Ponovno kliknite na gornji link za preuzimanje alata ESETSirefefCleaner.
5. Kada download završi pobrinite se da ponovno preimenujete naziv mape Windows Defender natrag na originalno ime. Kada završite, nastavite na dio II

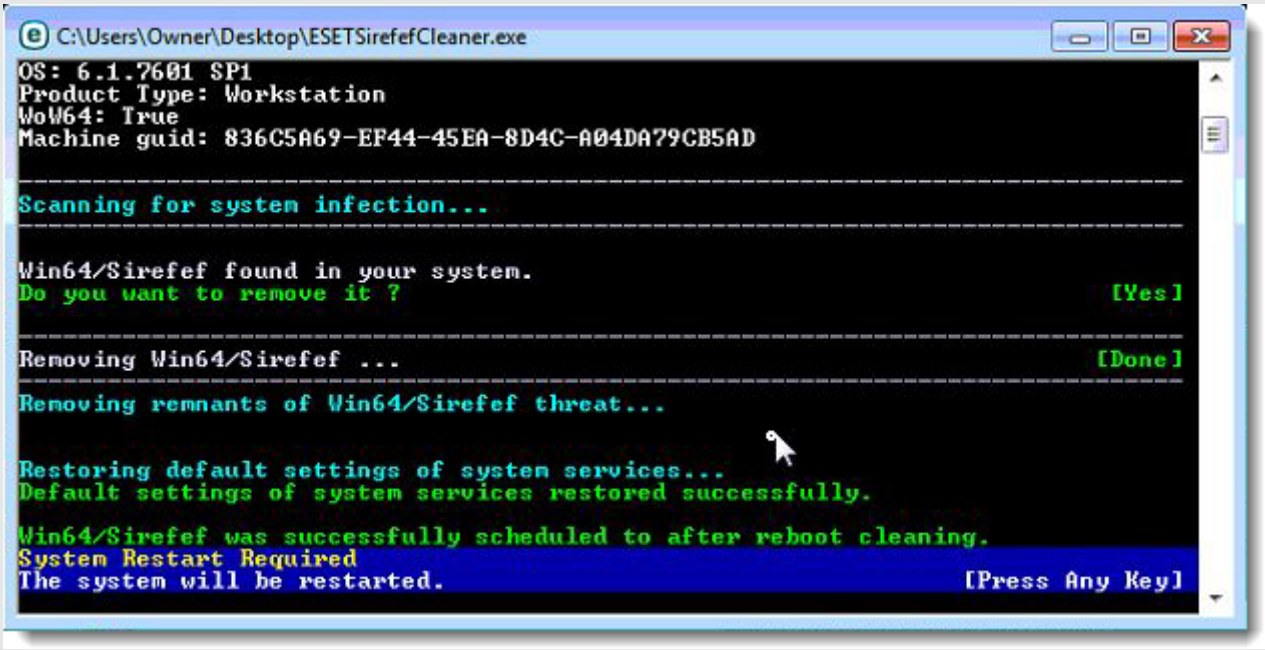
II Pokrenite ESETSirefefEVCleaner

1. Pronađite na Desktopu ESETSirefefEVCleaner (koji ste preuzeli u dijelu I), i pokrenite ga dvoklikom
2. Ako se pojavi sigurnosno upozorenje, kliknite na Continue ili Run.
3. Poruka “Win32/Sirefef.EV found in your system” bit će prikazana ako bude pronađena infekcija. Pritisnite slovo Y na vašoj tipkovnici kako bi uklonili infekciju.



Slika 1-1

4. Nakon završetka rada ovog alata i restarta računala, od vas će biti zatraženo da provedite povrat sistemskih servisa.
   Pritisnite slovo Y na vašoj tipkovnici da provedite povrat sistemskih servisa i ponovo restartate računalo.



Slika 1-2

5. Kada se računalo restarta, ako vam se pojavi sigurnosna obavijest kliknite na Yes ili Allow, potom nastavite na dio III ove upute

III Pokrenite prilagođeno skeniranje računala

Za detaljne upute o provođenju ovog skeniranja pročitajte ovaj članak baze znanja.

1. Otvorite glavni prozor ESET programa
2. Kliknite na Skeniranje računala Prilagođeno skeniranje...
   u postavkama tog skeniranja iz padajućeg menija Profil skeniranja odaberite Dubinsko skeniranje.
3. Kliknite na potvrdni okvir pokraj Computer pa kliknite na Skeniraj
   Za Windows XP: Kliknite na potvrdni okvir pokraj My Computer pa kliknite na Skeniraj.

Ovo skeniranje će ukloniti ostatke malicioznih programa još uvijek prisutne na računalu.

Ako nakon provođenja svih dijelova ovog postupka još uvijek uočavate problem, molimo kontaktirajte našu službu tehničke podrške.

IV Rješavanje problema

Ako nakon provođenja koraka u dijelovima I-III ovaj problem nije riješen, nastavite s niže navedenim uputama

1. Za Windows 8.1 i Windows 10:

   Pritisnite Windows tipku  + Q da pokrenete traženje aplikacija,
   u traku za pretraživanje upišite CMD,
   potom desnom tipkom miša kliknite na CMD i iz kontekstnog menija odaberite Run as administrator.
   Za Windows 7:

   Kliknite na Start  i u traku za pretraživanje upišite CMD.
   Desnom tipkom miša kliknite na CMD program i iz kontekstnog menija odaberite Run as administrator.
2. U komandnolinijskom okružju (CMD), utipkajte CD %userprofile%desktop pa pritisnite Enter.
   Direktorij će se promijeniti da indicira kako sada pristupate datotekama na Desktopu
3. Kako bi pokrenuli ESETSirefefCleaner alat u ručnom načinu rada za popravak, upišite komandu ESETSirefefCleaner.exe /r (pa pritisnite Enter).
   Sljedeći prekidači (engleski *switches*) mogu biti korišteni s ESETSirefefCleaner.exe:

   1. /d => Generira log: Skener će kreirati log aktivnosti koji može biti poslan ESET-u radi daljnjih analiza. Mi preporučujemo da koirstite taj prekidač kako bi naša služba podrške u slučaju potrebe mogla pregledati te logove.
   2. /s => Nevidljivi način rada (*engleski: Silent mode*): Datoteke će biti čišćene/dekriptirane u pozadini a log neće biti kreiran.
   3. /f =>Čišćenje na silu (*engleski: Force cleaning*): Svaka inficirana datoteka bit će očišćena/dekriptirana bez i jednog upita korisinku.
   4. /r => Vraćanje sistemskih servisa: Pokušati će se provesti povrat svih sistemskih komponenti koje su bile onemogućene ili oštećene djelovanjem malwarea.
4. Jednom kada ovaj alat završi djelovanje biti ćete upozoreni da trebate restartati računalo. kliknite Yes za restart.
5. Kada računalo izvrši restart, slijedite instrukcije iz dijela III ovog članka kako bi proveli prilagođeno skeniranje računala.

Ako nakon provođenja svih dijelova ovog postupka još uvijek uočavate problem, molimo kontaktirajte našu službu tehničke podrške.

Dodatne informacije i linkovi na povezane članke baze znanja

- Kako otvoriti ESET Smart Security ili ESET NOD32 Antivirus?
- Kako pokrenuti dubinsko skeniranje računala?
- Pogledajte video (na engleskom) o korištenju ESET Sirefef Cleaner alata

(posljednji puta revidirano 26.03.2020)

SOLN2895